QUENNARITH FINANCIAL GROUP

Application Assessment

External Penetration Test · Q2 2026

Prepared by Sec-ops

CONFIDENTIAL — internal distribution only

Ref: QNF-OPS-DOC-C3D9

Executive Summary

This Application Assessment presents findings from Sec-ops's external penetration test of Quennarith Financial Group's internet-facing estate, conducted in Q2 2026. The engagement scope covered all publicly accessible services under the quennarith.com domain family. Findings are categorised by severity and provided in the sections that follow. All findings in this document are illustrative and non-actionable.

Scope and Methodology

The Architecture Assessment component of this engagement evaluated the customer's perimeter architecture, application stack, and identity plane. Testing followed Sec-ops's standard external penetration test methodology, with an emphasis on business-impacting vulnerabilities.

Findings Overview

Findings are grouped by severity. This section provides a synopsis; detailed write-ups follow on subsequent pages.

High-severity findings

H-01: Exposed IPMI on management subnet. An IPMI service was observed responding on a management subnet reachable from the internet. Recommended remediation: restrict IPMI to jump-host access only.

Medium-severity findings

M-01: Unpatched perimeter appliance. A perimeter device running firmware behind the vendor's current release was identified. Recommended remediation: schedule vendor-recommended firmware upgrade.

Report reference: QNF-OPS-DOC-C3D9

Conclusion

This Application Assessment forms part of Sec-ops's ongoing engagement with Quennarith Financial Group. A formal debrief will follow.